

## Department of the Air Force, DoD

## § 806b.4

States citizens and permanent resident aliens.

(a) An official system of records must be:

(1) Authorized by law or Executive Order.

(2) Controlled by an Air Force or lower level directive.

(3) Needed to carry out an Air Force mission or function.

(b) The Air Force does not:

(1) Keep records on how a person exercises First Amendment rights. EXCEPTIONS are when: The Air Force has the permission of that individual or is authorized by federal statute; or the information pertains to an authorized law enforcement activity.

(2) Penalize or harass an individual for exercising rights guaranteed under the Privacy Act. Give reasonable aid to individuals exercising their rights.

(c) Air Force members:

(1) Keep paper and electronic records containing personal information and retrieved by name or personal identifier only in approved systems published in the FEDERAL REGISTER.

(2) Collect, maintain, and use information in such systems only to support programs authorized by law or Executive Order.

(3) Safeguard the records in the system and keep them the minimum time required.

(4) Keep the records timely, accurate, complete, and relevant.

(5) Amend and correct records on request.

(6) Let individuals review and receive copies of their own records unless the Secretary of the Air Force approved an exemption for the system or the Air Force created the records in anticipation of a civil action or proceeding.

(7) Provide a review of decisions that deny individuals access to or amendment of their records.

### § 806b.2 Violation penalties.

An individual may file a civil suit against the Air Force for failing to comply with the Privacy Act. The courts may find an individual offender guilty of a misdemeanor and fine that individual offender not more than \$5,000 for:

(a) Willfully maintaining a system of records that doesn't meet the public notice requirements.

(b) Disclosing information from a system of records to someone not entitled to the information.

(c) Obtaining someone else's records under false pretenses.

### § 806b.3 Personal notes.

If you keep personal notes on individuals to use as memory aids to supervise or perform other official functions, and do not share them with others, and an Air Force directive does not require their maintenance, the Privacy Act does not apply.

### § 806b.4 Responsibilities.

(a) The Administrative Assistant to the Secretary of the Air Force (SAF/AA) manages the entire program.

(b) The Office of the General Counsel to the Secretary of the Air Force (SAF/GCA) makes final decisions on appeals.

(c) The Director of Information Management (SAF/AAI), through the Access Programs Office of the Policy Division, (SAF/AAIA):

(1) Administers procedures outlined in this part.

(2) Submits system notices and required reports to the Defense Privacy Office.

(3) Guides major commands (MAJCOM) and field operating agencies (FOA).

(d) MAJCOM and FOA commanders, HQ USAF and Deputy Chiefs of Staff (DCS), and comparable officials, and SAF offices implement this part. Each HQ USAF and SAF office appoints a Privacy Act monitor. Send the name, office symbol, and phone number to SAF/AAIA.

(e) MAJCOM and FOA Information Managers:

(1) Manage the program.

(2) Appoint a command Privacy Act officer.

(3) Send the name, office symbol, and phone number to SAF/AAIA.

(f) Privacy Act Officers:

(1) Guide and train.

(2) Review the program at regular intervals.

(3) Submit reports.

(4) Review all publications and forms for compliance with this part.

## § 806b.5

- (5) Review system notices.
- (6) Investigate complaints.
- (7) Staff denial recommendations (at MAJCOMs and FOAs only).
- (g) System Managers:
  - (1) Decide the need for, and content of systems.
  - (2) Manage and safeguard the system.
  - (3) Train personnel on Privacy Act requirements.
  - (4) Protect records from unauthorized disclosure, alteration, or destruction.
  - (5) Prepare system notices and reports.
  - (6) Answer Privacy Act requests.
  - (7) Keep records of disclosures.
  - (8) Evaluate the systems annually.
- (h) Privacy Act Monitors (PAM):
  - (1) Are the focal point in their functional area for general Privacy Act questions and correspondence.
  - (2) Maintain a list of all systems of records and system managers in their area.
  - (3) Act as liaison with the Privacy Act Officer.
  - (4) Maintain statistics for the annual Privacy Act report.

## Subpart B—Obtaining Law Enforcement Records and Promises of Confidentiality

### § 806b.5 Obtaining law enforcement records.

The Commander AFOSI; the Chief, Air Force Security Police Agency (AFSPA); MAJCOM, FOA, and base chiefs of security police; AFOSI detachment commanders; and designees of those offices may ask another agency for records for law enforcement under 5 U.S.C. 552a(b)(7). The requesting office must indicate in writing the specific part of the record desired and identify the law enforcement activity asking for the record.

### § 806b.6 Promising confidentiality.

Record promises of confidentiality to exempt from disclosure any 'confidential' information under subsections (k)(2), (k)(5), or (k)(7) of the Privacy Act.

## 32 CFR Ch. VII (7–1–99 Edition)

## Subpart C—Collecting Personal Information

### § 806b.7 How to collect personal information.

Collect personal information directly from the subject of the record when possible. You may ask third parties when:

- (a) You must verify information.
- (b) You want opinions or evaluations.
- (c) You can't contact the subject.
- (d) The subject asks you.

### § 806b.8 When to give Privacy Act statements (PAS).

- (a) Give a PAS orally or in writing:

(1) To anyone from whom you are collecting personal information that will be put in a system of records.

(2) Whenever you ask someone for his or her Social Security Number (SSN).

NOTE: Do this regardless of how you collect or record the answers. You may display a sign in areas where people routinely furnish this kind of information. Give a copy of the PAS if asked. Do not ask the person to sign the PAS.

- (3) A PAS must include four items:

(i) Authority: The legal authority, that is, the United States Code or Executive Order authorizing the program the system supports.

(ii) Purpose: The reason you are collecting the information.

(iii) Routine Uses: A list of where and why the information will be disclosed outside DoD.

(iv) Disclosure: Voluntary or Mandatory. (Use Mandatory only when disclosure is required by law and the individual will be penalized for not providing information.) Include any consequences of nondisclosure in non-threatening language.

### § 806b.9 Requesting the social security number (SSN).

(a) Do not deny people a legal right, benefit, or privilege for refusing to give their SSNs unless the law requires disclosure, or a law or regulation adopted before January 1, 1975, required the SSN and the Air Force uses it to verify a person's identity in a system of records established before that date. When you ask for an SSN to create a record, tell the individual: